Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method of screening incoming packets, comprising:

detecting a request to establish a connection from a first network to a packet data network;

detecting establishment of a tunnel, wherein the tunnel has a support node at each end of the tunnel, one of the support nodes being a gateway to the packet data network, wherein the tunnel is used to convey user traffic and the user traffic through the tunnel can have one or more associated firewall sessions on a firewall outside the tunnel;

inspecting packets in the tunnel to detect information associated with the firewall sessions;

detecting a tear down of the tunnel in response to inspecting the packets; and

sending a request to the firewall to clear the one or more firewall sessions in response to detecting the tear down of the tunnel.[[.]]

2. (original) The method of claim 1, wherein:

detecting a tear down of the tunnel includes detecting the tear down of a GTP tunnel within the first network.

3. (original) The method of claim 1, further comprising:

stopping passage of packets to the first network originating from the packet data network and associated with a firewall session that is not on the firewall session list.

4. (original) The method of claim 1, further comprising:

dropping packets originating from the packet data network and not associated with a firewall session identifier on the firewall session list.

5. (original) The method of claim 1, wherein:

detecting the tear down of the tunnel includes detecting GTP delete tunnel request and response messages.

6. (original) The method of claim 1, further comprising:

clearing the one or more firewall sessions from a firewall session list.

7. (original) The method of claim 1, further comprising:

adding a firewall session to a firewall session list at a time when a new tunnel is created.

8. (canceled)

9. (currently amended) The method of claim [[8]] 1, wherein:

inspecting the packets in the tunnel includes determining at least one of a source address and a destination address of the packets in the tunnel.

10. (original) The method of claim 1, wherein:

detecting establishment of the tunnel includes determining the one or more firewall sessions associated with the tunnel.

11. (original) The method of claim 10, wherein:

detecting establishment of the tunnel includes determining two or more firewall sessions associated with the tunnel.

12-21. (canceled)

22. (currently amended) A system for screening incoming packets, comprising:

a GTP firewall ~~having~~ including a GTP communication module; and

a Gi firewall that includes: ~~having~~

a Gi communication module that is operable to receive an instruction from the GTP communication module to tear down a firewall session,

a firewall session list, and

a tear down engine that removes inactive firewall sessions from the firewall session list when the tear down engine receives the instruction from the GTP communication module.

23. (original) The system of claim 22, wherein:

the GTP firewall is operable to detect a GTP tunnel tear down.

24. (original) The system of claim 23, wherein:

the GTP firewall is operable to detect a firewall session end.

25. (original) The system of claim 22, wherein:

the GTP firewall includes a Gn firewall provided at a Gn interface.

26. (original) The system of claim 22, wherein:

the GTP firewall includes a Gp firewall provided at a Gp interface.

27. (original) The system of claim 22, wherein:

the GTP firewall is located on a device; and

the Gi firewall is located on the device.

28-31. (canceled)